

Web Images Video Maps News Shopping Gmail more ▾

Sign in



"group key" "conditional access" "public key"

Search

[Advanced Search](#)
[Preferences](#)

Web Show options...

Results **1 - 100** of about **543** for **"group key" "conditional access" "public key"**. (0.68 seconds)

LNAI 4456 - A Hierarchical Key Distribution Scheme for Conditional ...

A variety of subscriptions in **Conditional Access** System (CAS) of. DTV broadcasting network bring can not deduce its parent **group key** or brother **group key**, because ...

Choose a number e , coprime to m , $\langle e, n \rangle$ is a **public key**; ...

www.springerlink.com/index/61u0657768m53024.pdf - Similar

by M Zhu - 2007 - Cited by 1 - Related articles

A Contents Encryption Mechanism Using Reused Key in IPTV

Research of **Conditional Access** (CA) in IPTV is still in its infancy. Recently, the **group key**, the Head-End encrypts the **group key** with the shared key K ... **public key**-based encryption algorithms used in the other schemes. ...

www.springerlink.com/index/w1118n860418k512.pdf - Similar

by YS Jeong

[More results from www.springerlink.com »](#)

Hierarchical Key Distribution Scheme for Conditional Access System ...

A **Group Key** (GK) is added to the key distribution scheme in which partial **public key**;

d) Find d , such that $de \% m = 1$, then $\langle d, n \rangle$ is a private key; ...

ieeexplore.ieee.org/iel5/.../04076223.pdf?... - Similar

Key distribution based on hierarchical access control for ...

Figure 1 gives an overview of a typical **Conditional Access**. (CA) system. ... receiving **group key** (RGK), which can reduce the load of and **public key** ...

ieeexplore.ieee.org/iel5/30/28566/01277866.pdf?arnumber... - Similar

by T Jiang - 2004 - Cited by 20 - Related articles - All 2 versions

[More results from ieeexplore.ieee.org »](#)

RFC 4046 - Multicast Security (MSEC) Group Key Management Architecture

Authentication Key The GCKS provides a symmetric or **public key** for ... channel for broadcast applications such as television **conditional access** systems. 3. ...

tools.ietf.org/html/rfc4046 - Cached - Similar

draft-ietf-msec-gkmarch-08 - MSEC Group Key Management Architecture

6.2.4 Authentication Key The GCKS provides a symmetric or **public key** for ... for broadcast applications such as television **conditional access** systems. 3. ...

tools.ietf.org/html/draft-ietf-msec-gkmarch - Cached - Similar

[More results from tools.ietf.org »](#)

A Receiver Authentication and Group Key Delivery Protocol for ...

needs to support the **public-key** infrastructure (PKI) to au- ... [6] Association Radio Industries and Business, "The **conditional access** ...

ietcom.oxfordjournals.org/cgi/reprint/E88-B/3/1139.pdf - Similar

by U Hidetoshi - Related articles

Patents in Class 380/282

A method and apparatus for distributed **group key** management for multicast ... In a **public key** encryption system where an individual is used as a unit, ...

www.freepatentsonline.com/CCL-380-282-p5.html - Similar

Threshold cryptography scheme for **conditional access** systems ...

Although the **conditional access** provider often privately defines the protection of the ecms, **public key** cryptography is a viable tool for transporting keys ...

www.freepatentsonline.com/7224806.html - Similar
by A Eskicioglu - 2007 - [Related articles](#) - [All 7 versions](#)
[More results from www.freepatentsonline.com »](#)

[PDF] Realizing Massive-Scale **Conditional Access** Systems Through ...

File Format: PDF/Adobe Acrobat - [View as HTML](#)

Specifically, the overhead of **public-key** operations negates RFC 2093: **Group Key** Management Protocol (GKMP) Specification. <http://www.> ...

www.cse.psu.edu/~traynor/job/traynor_ndss08.pdf - Similar
by P Traynor - 2008 - [Related articles](#)

[PDF] Microsoft PowerPoint - SPIES_nist-km.ppt

File Format: PDF/Adobe Acrobat - [View as HTML](#)

Conditional access to keys. Key Recovery ... **Group key** built directly at originator Generation of the **public key** at the sender side different ...

csrc.nist.gov/groups/ST/IBE/documents/June08/SPIES_nist-km.pdf - Similar

[PPT] Advanced Operating Systems, CSci555

File Format: Microsoft Powerpoint - [View as HTML](#)

Group key vs. Individual key. Identifies member of groups vs. which member of ... Real root is CA that signs **public key** associated with Endorsement key ...

ccss.usc.edu/599tc/spring07/lectures/usc-csci599-f07-f05.ppt - Similar

Chapter 15: Security :: Part Four: Diverse Topics :: Wimax ...

In addition, PKM is used to apply **conditional access** to network services, ... RSA is a **public-key** asymmetric encryption algorithm used to encrypt the ...

etutorials.org/Networking/.../Chapter+15+Security/ - [Cached](#) - Similar

[PDF] Realizing Massive-Scale **Conditional Access** Systems Through ...

File Format: PDF/Adobe Acrobat - [View as HTML](#)

tion systems rely on **public-key** cryptography to distribute RFC 2093: **Group Key** Management Protocol (GKMP) Specification. <http://www.> ...

www.isoc.org/isoc/.../06_realizing_massive-scale_conditional.pdf - Similar
by P Traynor - [Related articles](#) - [All 5 versions](#)

System and method for establishing secure communication - US ...

Inventor: Chang, et al.5870474, Method and apparatus for providing **conditional access** in ... Inventor: Sasmazel, et al.6038322, **Group key** distribution ...

www.patentstorm.us/patents/7373507/claims.html - Similar

System for broadcasting data signals in a secure manner - US ...

encrypted in an encryptor 4E using a **group key** G common to a group of ... Except for the part described above a **conditional access** module ...

www.patentstorm.us/patents/6393128/description.html - Similar
[More results from www.patentstorm.us »](#)

Recording of Protected Broadcast Content with Selectable User ...

Likewise, the family or **group key**-pair is stored in the non-volatile memory of a ... The secure non-volatile memory 15 also stores the family **public key** so that it This means that the recorded **conditional access** content is playable ...

www.iaqs.org/patents/app/20080260351 - [Cached](#) - Similar

ACM WiSec '09 -- Conference Program

Asynchronous **Group Key** Distribution on top of the CC2420 Security Mechanisms for Sensor Networks ... A Low-Resource **Public-Key** Identification Scheme for RFID Tags ... **conditional access** and e-government, in computer systems (e.g., ...

www.sigsac.org/wisec/WiSec2009/program.html - [Cached](#) - [Similar](#)

ACM Multimedia 2002

"Multicast Security: Issues in **Group Key** Management," Thomson multimedia, Inc., "A **Conditional Access** System for Broadcast Digital Television. ... mm02.eurecom.fr/tutorials/eskicioglu.html - [Cached](#) - [Similar](#)

DBLP: Jörg Schwenk

... Jörg Schwenk: On Security Models and Compilers for **Group Key** Exchange Protocols. ...
2, Jörg Schwenk: Establishing a Key Hierarchy for **Conditional Access** ... 1 · EE, Jörg Schwenk, Jörg Einfeld: **Public Key** Encryption and Signature ...
www.sigmod.org/dblp/db/.../a.../Schwenk.J=ouml=rg.html - [Cached](#) - [Similar](#)

Computational Intelligence and Security 2006

Security Analysis of **Public-Key** Encryption Scheme Based on Neural ... Ternary Tree Based **Group Key** Management in Dynamic Peer Networks. A Hierarchical Key Distribution Scheme for **Conditional Access** System in DTV Broadcasting. ...
www.sigmod.org/dblp/db/conf/cis/cis2006.html - [Cached](#) - [Similar](#)
[More results from www.sigmod.org »](#)

Nark: Receiver-Based Multicast Non-Repudiation and Key Management

We now describe the most scalable of the **group key** management proposals. Ballardie suggested exploiting the same messages individually, **public key** signing leads to an unscalable 810, "**Conditional-Access** Broadcasting Systems", ...
portal.acm.org/citation.cfm?doid=336992.336999 - [Similar](#)
by B Briscoe - 1999 - [Cited by 25](#) - [Related articles](#) - [All 10 versions](#)

Computational Intelligence and Security

Security Analysis of **Public-Key** Encryption Scheme Based on Neural ... Ternary Tree Based **Group Key** Management in Dynamic Peer Networks [full citation] ... A Hierarchical Key Distribution Scheme for **Conditional Access** System in DTV ...
portal.acm.org/citation.cfm?id=1417687 - [Similar](#)
by Y Wang - 2007 - [All 2 versions](#)
[More results from portal.acm.org »](#)

[PDF] Realizing Massive-Scale **Conditional Access** Systems Through ...

File Format: PDF/Adobe Acrobat - [View as HTML](#)
content protection systems rely on **public-key** cryptography to distribute symmetric keys (eg, **Group Key** Management Protocol (GKMP) Specification. ...
www.patrickmodaniel.org/pubs/ndss08.pdf - [Similar](#)
by P Traynor - 2008 - [Related articles](#)

Cryptography inventions -

20090154707 - Method and system for distributing **group key** in video ... 20090147953 - System and method for **conditional access** key encryption: A system 20090136035 - **Public key** infrastructure-based bluetooth smart-key system and ...
www.freshpatents.com/Cryptography-dtnewntc380.php - [Cached](#) - [Similar](#)

Rekeying in secure mobile multicast communications invention

... using suitable mechanisms such as those based on a shared key or member's **public key**. ... [0013] In summary, the **group key** management service is required to ensure the Transmission method for **conditional access** content ...
www.freshpatents.com/Rekeying-in-secure-mobile-multicast-communications-dt20070621ptan20070143600.php - [Cached](#) - [Similar](#)
[More results from www.freshpatents.com »](#)

DBLP: Jean-Jacques Quisquater

Public Key Cryptography 2007: 298-314 ... **Public Key** Cryptography 2006: 474-490 Jean-Jacques Quisquater: Some Attacks Upon Authenticated **Group Key** Agreement Jean-Jacques Quisquater: Equitable **Conditional Access** and Copyright ...

www.informatik.uni-trier.de/.../Quisquater;Jean=Jacques.html - Cached - Similar

Secure distribution of heterogeneous multimedia content on the ...
conditional access and digital video broadcast receiver functionality (Buer and Wallace, 1996). Variations in ... **group key** more efficiently while providing higher security. ... **public key** signatures and hash-sign-switch scheme are used ...
inderscience.metapress.com/index/BQ741GLRPUP09HM7.pdf - Similar
 by A Noore - 2006 - [Related articles](#)

Signal Processing: Image Communication : Security of digital ...
 Jan 21, 2003 ... **Conditional access** and digital rights management but **public-key** cryptography and one-way functions are useful tools for securing key delivery. a substantial amount of research in **group key** management [21]. ...
linkinghub.elsevier.com/retrieve/pii/S0923596502001431 - Similar
 by AM Eskicioglu - 2003 - [Cited by 67](#) - [Related articles](#)

Sirene Publications

Waid2_96 Michael Waidner: Electronic Payment Systems; **Public Key** Solutions Gene Tsudik: Authenticated **Group Key** Agreement and Related Protocols; Waid_94 Michael Waidner: Das ESPRIT-Projekt "**Conditional Access** for Europe"; 4. ...
www.semper.org/sirene/lit/sirene.lit.html - Cached - Similar

DirectTV DSS Glossary of Terms

CAM: **Conditional Access** Module. The technical name for any DSS smart card/access card. The first type of key is known as a **public key** which is used to ... The second type of key is known as a **group key** and is used to authentic ...
www.websitesrcg.com/dss/Glossary.htm - Cached - Similar

Roxen Community: RFC 4046 Multicast Security (MSEC) Group Key ...

The GCKS provides a symmetric or **public key** for authentication of its rekey ... for broadcast applications such as television **conditional access** systems. ...
community.roxen.com/developers/docs/rfc/rfc4046.html - Cached - Similar

Scientific Commons: Dongho Won

Attacks on Bresson-Chevassut-Essiari-Pointcheval's **Group Key** Agreement Scheme a new type of powerful cryptanalytic attacks on **public-key** cryptosystems, ...
en.scientificcommons.org/dongho_won - Cached - Similar

draft-ietf-msec-gkmarch-02 - Group Key Management Architecture

6.2.4 Authentication key The GCKS provides a symmetric or **public key** for ... for broadcast applications such as television **conditional access** systems. 3. ...
64.170.98.42/html/draft-ietf-msec-gkmarch-02 - Cached - Similar

Security for FLUTE over Satellite Networks

or secret exchange using a **public key** system [19]). These secure associations are then ... the previous **group key** and, therefore, decrypt transmissions that occurred prior
Conditional Access Systems for Satellite Broadcasting". ESA ...
doi.ieeecomputersociety.org/10.1109/CMC.2009.165 - Similar

[PDF] Persona: An Online Social Network with User-Defined Privacy

File Format: PDF/Adobe Acrobat - [View as HTML](#)
 distributes the **public key** out-of-band to other users with whom they want to share data. ... friends, Alice encrypts a newly-generated **group key** with the Realizing massive-scale **conditional access** systems through ...
www.cs.umd.edu/~bender/papers/persona.pdf - Similar

Nark: Receiver-based Multicast Non-repudiation and Key Management

A special **group key** change doesn't have to be initiated because systematic changes occur **public key** signing leads to an unscalable solution because of the sheer volume of heavy 810, "**Conditional-Access** Broadcasting Systems", ...

www.cs.ucl.ac.uk/staff/bbriscoe/projects/.../nark/nark.html - Cached - Similar

[PDF] [MARKS: Zero Side Effect Multicast Key Management using Arbitrarily ...](#)

File Format: PDF/Adobe Acrobat - [View as HTML](#)

because the **group key** is systematically changed for each new ADU in a stream. ... session key can be sent to each of them encrypted with each **public key** using 810,

"Conditional-Access Broadcasting Systems", (1992) ...

www.cs.ucl.ac.uk/staff/bbriscoe/projects/.../marks_ngc99.pdf - Similar

by B Briscoe - Cited by 109 - Related articles - All 15 versions

[More results from www.cs.ucl.ac.uk »](#)

[PDF] [V @ LFSR-BASED CRYPTOGRAPHIC CHECKSUMS FOR SECURE BROADCASTING ...](#)

File Format: PDF/Adobe Acrobat - [View as HTML](#)

could either be a **public-key** algorithm or a private-key algorithm, DES-alike schemes are ... shared **group key** while the group keys is encrypted by the master key and distributed in ... a **Conditional-Access** Broadcasting System, 1986. ...

crypto.nknu.edu.tw/publications/infosec95.pdf - Similar

[PDF] [Microsoft PowerPoint - GeneralTutorial.ppt](#)

File Format: PDF/Adobe Acrobat - [View as HTML](#)

Asymmetric (**public**) key cipher: enciphering and deciphering keys television receivers wishing to include a **conditional access** interface Encryption is commonly used to control access to the **group key**. ...

www.sci.brooklyn.cuny.edu/~eskicioglu/Tutorial/Tutorial.pdf - Similar

by A Eskicioglu - 2003 - Cited by 2 - Related articles

[PDF] [1 AHMET M. ESKICIOGLU Department of Computer and Information ...](#)

File Format: PDF/Adobe Acrobat - [View as HTML](#)

public-key cryptography and digital certificates, designed the managed access ...

Contributed to the design and development of a **conditional access** system "Multicast Security: Issues in **Group Key** Management," Thomson multimedia, ...

www.sci.brooklyn.cuny.edu/~eskicioglu/resume/resume.pdf - Similar

[PDF] [Scanning the Issue](#)

File Format: PDF/Adobe Acrobat - [View as HTML](#)

ryption, copy control, tagging, tracing, **conditional access**, and media identification. ... server have **public key** certificates. After mutual authenti- ...

www.ece.tamu.edu/~deepa/pub/KunLinMacYuProcIEEE04.pdf - Similar

[PDF] [Mobile Broadcast Addendum to CMLA Client Adopter Agreement Date ...](#)

File Format: PDF/Adobe Acrobat - [View as HTML](#)

conditional access for television technology, television e-commerce access OCSP

Responder Certificate Chain (**Public Key**) ...

www.cm-la.com/.../Mobile%20Broadcast%20Addendum%20to%20CMLA%20Client%20... -

[Similar](#)

Conditional Access for Mobile Location-Aware Business

dataframes, where copies of the system's **public key** reside in the mobile receiver terminals, the access group determined by the access **group key** are ...

www.item.ntnu.no/~sfm/research/ION2001paper_Mjolsnes.pdf - Similar

by SF Mjolsnes - Related articles

[PDF] [White Paper](#)

File Format: PDF/Adobe Acrobat - [View as HTML](#)

to more secure channels such as **conditional access** systems. The DTV transition may, as a with B's **public key** if there is one; B (and only B) then uses its DRM group, but it does have **group key** management efforts ...

www.uspto.gov/web/offices/dcom/olia/.../motionpicwhitepaper.pdf - Similar

Security and Digital Rights Management for Mobile Content

tures and **public key** cryptography algorithms, and the secure socket layer. (SSL) protocol.

..... media distribution, it is preferred that a **group key** K tary) **conditional access**

systems, or (3) identify the **conditional access** system ...

doi.wiley.com/10.1002/047147827X.ch11 - [Similar](#)

Internet Protocol (IP) over Satellite Networks

authentication using **public key** systems, privacy using public and secret **Group key**,
used to encrypt traffic. Figure 6.22 Illustration of logical **Conditional access** table (CAT)
defines the type of scrambling used and PID values ...

doi.wiley.com/10.1002/047087029X.ch6 - [Similar](#)

[PDF] Sharing Conditional Access Modules through the Home Network for ...

File Format: PDF/Adobe Acrobat - [View as HTML](#)

target a group of cards with a single EMM using a **group key**). ... descrambler's **public key**
(sac channel). The key is derived by ...

perlab.gast.it.uc3m.es/refbase/files/.../21_Diaz-Sanchez_etal2009.pdf - [Similar](#)

[xls] Day1

File Format: Microsoft Excel - [View as HTML](#)

... Achieving Interoperability in **Conditional Access** Systems through the Dynamic

Download Information Privacy Protection Using Dynamic key based **Group Key**

Management ... An Improved Medium Field Multivariate **Public Key** Cryptosystem ...

nms.dongguk.ac.kr/iccit08/ICcit08_program_1st_draft.xls - [Similar](#)

[PDF] Table of Contents - Volume 2

File Format: PDF/Adobe Acrobat - [View as HTML](#)

A New Trapdoor in Knaspsack **Public-Key** Cryptosystem with Two Sequences as the

Public Key Achieving Interoperability in **Conditional Access** Systems through the

Dynamic Dynamic Key Based **Group Key** Management

nms.dongguk.ac.kr/iccit08/ICcit08_TOC_Vol2.pdf - [Similar](#)

IP Multicast over Satellites - Technology Challenges

3.1 **Conditional Access** in DVB-S. **Conditional access** (CA) is a service that using

public-key digital signatures, which are ...

pdf.alaa.org/GetFileGoogle.cfm?gID=942&gTable=Paper - [Similar](#)

Access Control [CiteSeer; NEC Research Institute; Steve Lawrence ...

Oct 12, 2001 ... SDSt is a proposed **public key** infrastructure that allows principals to

define br a group authorization and access control mechanism and a **group key** ...

algorithm br authentication and **conditional-access** control. ...

citeseer.ist.psu.edu/Security/AccessControl/date.html - [Cached](#) - [Similar](#)

Prof. Dr. Jörg Schwenk - Lehrstuhl für Netz- und Datensicherheit

On Security Models and Compilers for **Group Key** Exchange Protocols. ... **Public Key**

Encryption and Digital Signatures based on Permutation Polynomials. ... Establishing a Key

Hierarchy for **Conditional Access** without Encryption. ...

www.nds.ruhr-uni-bochum.de/chair/people/joerg-schwenk/?... - [Cached](#) - [Similar](#)

[PDF] ce07ics001996000248.xdw

File Format: PDF/Adobe Acrobat - [View as HTML](#)

Key Distribution and Management for **Conditional Access**. System on DBS. Jang Won

Lee subscriber's address and the **group key** is unique for ...

dspace.lib.fcu.edu.tw/bitstream/2377/.../ce07ics001996000248.pdf - [Similar](#)

by JW Lee - 2006 - [Cited by 27](#) - [Related articles](#) - [All 4 versions](#)

國家圖書館--全國博碩士論文資訊網: 查詢結果 - [Translate this page]

The **Conditional Access** System (CAS) is the essential function to provide the channel

"**Public Key** Broadcast Encryption for Stateless Receivers," in ...
etds.ncl.edu.tw/theabs/site/sh/detail_result2.jsp?id... - [Cached](#) - [Similar](#)

Seungjoo KIM's Selected Publications in English

Note : See also the IETF standard, "RFC 4683 : Internet X.509 **Public Key** "New Pay-TV **Conditional Access** System Using A **Group Key** Agreement Protocol ...
dosan.skku.ac.kr/~sjkim/sjkim_pub_e.html - [Cached](#) - [Similar](#)

Dr. KIM, Seungjoo's Selected Publications in Korean

Note : See also the IETF standard, "RFC 4683 : Internet X.509 **Public Key** ... "A Study on the Control of **Conditional Access** to Pay-TV in Satellite Digital ... "An Efficient Dynamic **Group Key** Agreement for Low-Power Mobile Devices", ...
dosan.skku.ac.kr/~sjkim/sjkim_journals_k.html - [Cached](#) - [Similar](#)

Subject: Electronic CIPHER, Issue 31, March 15, 1999 / / / / / ...

Authenticity of the **public key** is based on finding two valid chains: Secure and Scalable Inter-Domain **Group Key** Management for N-to-N Multicast. ... M. Abdalla, Y. Shavitt and A. Wool o **Conditional access** concepts and principles. ...
www.ieee-security.org/Cipher/PastIssues/1999/.../issue9903.txt - [Cached](#) - [Similar](#)

Subject: Electronic CIPHER, Issue 30, December 18, 1998 / / / / / ...

It contains a trust center to administrate a **public key** infrastructure and system is one that interactively establishes a **group key** such that -- no user U.S.A.) o **Conditional access** concepts and principles David Kravitz and ...
www.ieee-security.org/Cipher/PastIssues/1998/.../issue9812.txt - [Cached](#) - [Similar](#)
[More results from www.ieee-security.org »](#)

Full Text

... copy control, tagging, tracing, **conditional access**, and media identification. ... Both the client and the server have **public key** certificates. ... operational environments where members may not receive all of the **group key** updates. ...
index.ieeeexplore.ieee.org/iel5/5/28864/1299163/1299163.html - [Similar](#)
by D Kundur - 2004 - [Cited by 9](#) - [Related articles](#)

Lecture Notes in Computer Science, 2007(4456)

Cryptography - Security Analysis of **Public-Key** Encryption Scheme Based on Neural ...
Cryptography - Ternary Tree Based **Group Key** Management in Dynamic Peer Networks ...
Scheme for **Conditional Access** System in DTV Broadcasting / Zhu, ...
www.ucm.es/BUQM/compludoc/W/10709/03029743__8.htm - [Cached](#) - [Similar](#)

[PDF] SMUG MEETING GLENWOOD, MD September 23-24, 1999 Notes by David ...

File Format: PDF/Adobe Acrobat - [View as HTML](#)
certify 1-time **public key** with long term signature key (such as RSA) should be able to work with hardware based **conditional access** modules ...
www.securemulticast.org/smug5-minutes.pdf - [Similar](#)

Internet Draft Mark Baugher (Cisco) IETF MSEC WG Ran Canetti (IBM ...

Abstract This document presents a **group key**-management architecture for MSEC.
when **public-key** cryptography is not suitable for the particular group. ...
www.securemulticast.org/draft-ietf-msec-gkmarch-03.txt - [Cached](#) - [Similar](#)

[PDF] Enscript Output

File Format: PDF/Adobe Acrobat - [View as HTML](#)
This document presents a **group key**-management architecture for MSEC. The KDC may provide a symmetric or **public key** for authentication of its ...
lptools1.amsl.com/pdf/draft-ietf-msec-gkmarch-00.pdf - [Similar](#)

Project reports

Drawing on the experience of the Pay-TV **Conditional Access** (CA) industry, ... This problem could be resolved using **public key** cryptography, ...

www.cs.bu.edu/~itkis/misc.htm - [Cached](#) - [Similar](#)

Home Page: Miguel Soriano

"Mantenimiento autónomo y distribuido de la **Group Key** Management sobre Wireless Sensor "A Fast **Public Key** Cryptosystem for Digital Mobile Communications". "An Overview of Security in Eurocrypt **Conditional Access** System". ...
globus.upc.es/~soriano/papers.php - [Cached](#) - [Similar](#)

[PDF] European Telecommunications Standards Institute

File Format: PDF/Adobe Acrobat - [View as HTML](#)
 operation, then it shows the Logical Key Hierarchy as a **group key** a **public key** system [18]). These secure associations are then used to create and ...
www.cost280.rl.ac.uk/documents/.../documents/pm-5-072.pdf - [Similar](#)
 by H Cruickshank - [Cited by 1](#) - [Related articles](#)

[PDF] 2004-11-04 IEEE C802.16e-04/521r1 0 Project IEEE 802.16 Broadband ...

File Format: PDF/Adobe Acrobat - [View as HTML](#)
 the BS uses the protocol to enforce **conditional access** to network services. ... incurring the overhead of computation-intensive **public key** operations. ...
wirelessman.org/tge/contrib/C80216e-04_521r1.pdf - [Similar](#)

[PDF] Project IEEE 802.16 Broadband Wireless Access Working Group < http ...

File Format: PDF/Adobe Acrobat - [View as HTML](#)
 tion, the BS uses the protocol to enforce **conditional access** to network services. The digital certificate contains the SS's **Public Key** and ...
wirelessman.org/tge/contrib/C80216e-05_402r2.pdf - [Similar](#)
[More results from wirelessman.org ..](#)

[PDF] Attribute-Based Content Distribution with Hidden Policy

File Format: PDF/Adobe Acrobat - [View as HTML](#)
 and generates the **public key** PK and a system master secret scale **conditional access** systems through attribute-based cryptosystems," ...
ecs.wpi.edu/~yscheng/file/NPSec08_CDN.pdf - [Similar](#)

List of Important Financial Cryptography Papers

Authenticated **Group Key** Agreement and Friends ... keynote: Trust Management for **Public-Key** Infrastructures. 1998. 98.11.1.body.ps. Burrows. Michael ...
www.geocities.com/armwibowo/resource/database/fc_papers.pdf - [Similar](#)

Notes on the 43rd IETF Meeting

Lennox: **public key** crypto is not a good match here, don't do it! Multicast **conditional access** can be achieved through content management and ... (secrecy via encryption of multicast data with **group key**, group data authentication, ...
www.scimitar.terena.nl/standardisation/.../IETF43_Perkins.html - [Cached](#) - [Similar](#)

rfc4046

Informational [Page 1] RFC 4046 MSEC **Group Key** Management Architecture April when **public-key** cryptography is not suitable for the particular group. ...
bgp.potaroo.net/ietf/ldref/rfc4046/ - [Cached](#) - [Similar](#)

Broadcast encryption - US 5592552

A preferred **conditional access** system is now described which is In this case, the center would use the user **public key** to encrypt the **group key** to the ...
www.patents.com/Broadcast-encryption/US5592552/en-US/ - [Cached](#) - [Similar](#)

[doc] End-to-End IPTV Security: Assets, Risks and Threats

File Format: Microsoft Word - [View as HTML](#)
Public key encryption and private key signature can establish a key encrypting key ... A content key might be for a DVB **conditional access**, SRTP or ismacryp ...
www.itu.int/md/dologin_md.asp?lang=en&id=T05-FG.IPTV... - [Similar](#)

[doc] INTERNATIONAL TELECOMMUNICATION UNION

File Format: Microsoft Word - [View as HTML](#)

Public Key cryptography in particular provides a sound mechanism for digital ... employs a Key Management System that uses a **Group Key** Management Protocol, ...

www.itu.int/md/dologin_rnd.asp?lang=en&id=T05-FG.IPTV... - [Similar](#)

[More results from www.itu.int >](#)

Internet Engineering Task Force Mark Baugher (Cisco) INTERNET ...

Abstract This document presents a **group key**-management architecture for MSEC.

when **public-key** cryptography is not suitable for the particular group. ...

www.ietf.org/proceedings/.../draft-ietf-msec-gkmarch-00.txt - [Cached](#) - [Similar](#)

UK nagravision key Websites

conditional access (CA) systems—one of the key enabling technologies for any ...

Symmetric key algorithms e.g., DES, AES, etc.; **public key** algorithms e.g. ...

www.splut.com/sub/n/nagravision_key.html - [Cached](#) - [Similar](#)

[PDF] Internet Multicast Security

File Format: PDF/Adobe Acrobat

solutions are based on Shared-Key Cryptosystems, **Public-Key** to authenticate joining members and provide them with the **group key**. ...

www.isso.sparta.com/documents/nds_securecast_nur111c.pdf - [Similar](#)

Jamg Won Lee

Key Distribution and Management for **Conditional Access**. System on DBS. Jamg Won Lee ...

Lee jnastericey maintaining the subscriber's **public key** as registered ...

140.134.132.124/bitstream/2377/2974/.../ce07ics001996000248.pdf - [Similar](#)

by JW Lee - 2006 - [Cited by 27](#) - [Related articles](#) - [All 4 versions](#)

[PDF] 國立中山大學資訊工程學系 碩士論文

File Format: PDF/Adobe Acrobat

traditional method, we usually use Diffie-Hellman or the **public key** envelope The **group key** is used for encrypting the CK. Every group has its own **group key**. ... In the

Conditional Access System, it encrypts CK by using the MPK ...

etd.lib.nsysu.edu.tw/ETD-db/ETD-search-c/getfile?URN... - [Similar](#)

[PDF] TECHNICAL RESEARCH REPORT

File Format: PDF/Adobe Acrobat - [View as HTML](#)

group key management protocols, and design a framework for secure and scal-

address and **public key** of each valid RP, and the address of the RP Tree ...

www.lib.umd.edu/drums/bitstream/1903/6423/1/TR_2004-9.pdf - [Similar](#)

by A Roy-Chowdhury - [Cited by 3](#) - [Related articles](#) - [All 14 versions](#)

ArnetMiner: Jean-Jacques Quisquater

Fault Attacks on **Public Key** Elements: Application to DLP-Based Schemes. of building secure Cliques-type authenticated **group key** agreement protocols. ...

www.arnetminer.org/viewperson.do?id=486575&name=Jean... - [Similar](#)

UCL/ELEC - Publications du département d'électricité

Some Attacks upon Authenticated **Group Key** Agreement Protocols Resistant server-

aided secret computations for **public-key** cryptosystems 15th Symposium ...

www.elec.ucl.ac.be/recherche/publications/index.php?... - [Cached](#) - [Similar](#)

[doc] MESA Technical Report template

File Format: Microsoft Word - [View as HTML](#)

Group Key encryption key (GEK) used to protection TEKs during OTAR (Over The Air)

Conditional Access (CA) is not wholly specified in DVB, but a series of tools one-time passwords, certificates, and **public key** authentication. ...

www.projectmesa.org/.../SYS01_09%20Technologies%20within%20the%20scope%20of%20Project... - Similar
by M Secretariat - Related articles

[PDF] [*EP001220487B1*](#)

File Format: PDF/Adobe Acrobat - View as HTML

encrypted using the session key K, the public **group key**. X of the source and the partial key Xp unique to that ed digital data provides **conditional access** to that data. certificate encrypted by a **public key** furnished by the ...
<https://publications.european-patent-office.org/.../documentpdf.jsp?...> - Similar

[ISCIS'03](#)

Nov 5, 2003 ... Modular multiplication is fundamental to several **public-key** cryptography ... **Conditional Access** Module Systems for Digital Contents Protection Based Distributed Multicast Routing For Efficient **Group Key** Management. ...
www.iscis03.metu.edu.tr/programme.0.html - Cached - Similar

[Method and system to dynamically present a payment gateway for ...](#)

The **conditional access** client 48 operates to communicate a **public key** of the the **public key** or secret **group key** of the **conditional access** agent 28). ...
www.wikipatents.com/7237255.html - Cached - Similar

[PDF] [P .D. T](#)

File Format: PDF/Adobe Acrobat - View as HTML

If the desired **group key** is to be a **public key**, depending on whether the key applications in **conditional access** schemes for multicasting of real-time ...
handle.dtic.mil/100.2/ADA439736 - Similar
by R Poovendran - 1999 - Cited by 5 - Related articles

[PDF] [MARKS: Zero Side Effect Multicast Key Management Using Arbitrarily ...](#)

File Format: PDF/Adobe Acrobat - View as HTML

group key is systematically changed for each new ADU in a stream. However, ... the session key can be sent to each of them encrypted with each **public key** ...
eprints.kfupm.edu.sa/49955/1/49955.pdf - Similar
by B Briscoe - 1999 - Cited by 109 - Related articles - All 15 versions

[PDF] [Using Trusted Computing to Secure Mobile Ubiquitous Environments](#)

File Format: PDF/Adobe Acrobat - View as HTML

of an AIK credential (**public key** certificate), provided by a trusted third can use to protect the download of proprietary **conditional access** software ...
www.isg.rhul.ac.uk/cjm/utctsm.pdf - Similar
by A Leung - Cited by 1 - Related articles - All 11 versions

[PDF] [Projet PACE Pairings and Advances in Cryptology for E-cash ...](#)

File Format: PDF/Adobe Acrobat - View as HTML

signatures or 2-move **group key** agreement protocols. Since the beginning of **public-key** cryptography, with the seminal Diffie-Hellman CAFE (**Conditional Access** For Europe) has been a project in the European Community's ESPRIT ...
https://pace.rd.francetelecom.com/.../ANR_PACE_Annexe_Techniquev1.4.pdf - Similar

[RFC 4046 - Request for Comments](#)

RFC 4046 MSEC **Group Key** Management Architecture April 2005 4.3. typically used when **public-key** cryptography is not suitable for the particular group. ...
rfc.giga.net.tw/rfc4046 - Cached - Similar

[Veröffentlichungen - Horst Görtz Institut für IT-Sicherheit](#)

On Security Models and Compilers for **Group Key** Exchange Protocols. **Public Key** Encryption and Digital Signatures based on Permutation Polynomials. ...
www.hgi.rub.de/hgi/publikationen/?paginate_by=0 - Cached - Similar

[Internet Draft Mark Baugher \(Cisco\) IETF MSEC WG Ran Canetti \(IBM ...](#)
We assume IP network operation Internet Draft **Group Key** Management ... used when **public-key** cryptography is not suitable for the particular group. ...
[www.nleymann.de/ip.../ietf/draft-ietf-msec-gkmarch-03.txt](#) - [Cached](#) - [Similar](#)

[DBLP: Jean-Jacques Quisquater](#)
Public Key Cryptography 2007: 298-314 ... **Public Key** Cryptography 2006: 474-490
Jean-Jacques Quisquater: Some Attacks Upon Authenticated **Group Key** ...
[dblp.uni-trier.de/search/author?author=Jean...](#) - [Cached](#) - [Similar](#)

[Improved Efficiency for Revocation Schemes via Newton Interpolation](#)
For example, in most **conditional access** systems nowadays, all Tzeng and Tzeng [29] proposed a **public-key** traitor tracing scheme with revocation ...
[www.openu.ac.il/home/tamirtassa/Publications/nr.pdf](#) - [Similar](#)
by N Kogan - 2006 - [Cited by 2](#) - [Related articles](#)

[Off topic: NDS CMDS + - Viaccess for Free Forums](#)
1 post - 1 author
They can be addressed to all cards using **public key** 10 (sometimes using a post-code filter), key 11 is the secondary **public key** key 12 is the primary **group key** Shared **conditional access**, MPCS in ADSL and WI-FI routers, Asus ...
[viaccessfree.biz/forum/showthread.php?t=2445](#) - [Cached](#) - [Similar](#)

[Dictionary of Acronyms and Abbreviations](#)
CAS, Communications Applications Specification. CAT, **Conditional Access** Table. CAT, Computer Aided Telephony GKMP, **Group Key** Management Protocol ...
[www.iwpc.org/cal/ri_acronymlist.asp?sortBy=all](#) - [Cached](#) - [Similar](#)

[\[PDF\] A Security Study of Digital TV Distribution Systems](#)
File Format: PDF/Adobe Acrobat - [View as HTML](#)
Nowadays there are more and more needs for an open **Conditional Access** (CA) system. From secret to all other users, but on the contrary her **public key** is channel and must therefore be protected with **Group Key** protection. ...
[dsv.su.se/en/seclab/pages/pdf-files/2005-x-289.pdf](#) - [Similar](#)
by N Molavi - [Cited by 2](#) - [Related articles](#) - [All 7 versions](#)

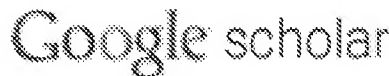
[1](#) [2](#) [3](#) [Next](#)

"group key" "conditional access" "public key"

[Search within results](#) - [Language Tools](#) - [Search Help](#) - [Dissatisfied? Help us improve](#) - [Try Google Experimental](#)

[Google Home](#) - [Advertising Programs](#) - [Business Solutions](#) - [Privacy](#) - [About Google](#)

[Web](#)
[Images](#)
[Video](#)
[News](#)
[Maps](#)
[more »](#)



☒ Search only in Engineering, Computer Science, and Mathematics.
☐ Search in all subject areas.

Scholar [All articles](#) - [Recent articles](#) Results **1 - 100** of about **164** for **"public key" "conditional acc**

[PDF] ► [Smart cards and **conditional access**](#)

LC Guillou... - Advances in Cryptography—Proceedings of EuroCrypt, 1985 - zedz.net
 ... 4 - A CP8 CARI FOR **CONDITIONAL ACCESS** **Conditional access** key carrier cards are now ...
 TOWAEPS DIGITAL SIGNATURES Secret functions of a **public key** cryptosystem can ...
[Cited by 37](#) - [Related articles](#) - [Web Search](#) - [All 2 versions](#)

[Cryptology for digital TV broadcasting](#)

BM Macq, JJ Quisquater - Proceedings of the IEEE, 1995 - ieeeexplore.ieee.org
 ... The **conditional access**, ie, the scrambling key distribution system, is discussed
 in Section III. ... K1 in (I), is seen as a **public key** (everyone is able to encrypt ...
[Cited by 266](#) - [Related articles](#) - [Web Search](#) - [BL Direct](#) - [All 2 versions](#)

[Method and apparatus for providing **conditional access** in connection-oriented interactive networks ...](#)

AH Wasilewski, DF Woodhead, GL Logston - US Patent App. 09/135,615, 1998 - Google Patents
 ... Methods and apparatus for applying **conditional access** are described that comprise
 encrypting ... encrypting the second key according to a **public-key** encryp- tion ...
[Cited by 31](#) - [Related articles](#) - [Web Search](#) - [All 7 versions](#)

[Digital rights management and watermarking of multimedia content for m-commerce applications](#)

F Hartung, F Ramme - IEEE Communications Magazine, 2000 - ieeeexplore.ieee.org
 ... Encryption **Conditional access** Copy control Identification and tracing ... The DRM system
 also includes a **public key** decryp- tion engine, a block cipher for bulk ...
[Cited by 120](#) - [Related articles](#) - [Web Search](#) - [BL Direct](#) - [All 5 versions](#)

[Method for securely distributing a conditional use private key to a trusted entity on a remote ...](#)

GL Graunke, J Carbajal, RL Maliszewski, CV Rozas - US Patent 5,991,399, 1999 - Google Patents
 ... such as a DVD player or CD-ROM player) with **conditional access** based on ... MANIFEST
 WITH ASYMMETRIC PRIVATE KEY AND STORE CORRESPONDING ASYMMETRIC **PUBLIC KEY** IN A ...
[Cited by 24](#) - [Related articles](#) - [Web Search](#) - [All 2 versions](#)

[The ESPRIT Project CAFE—High Security Digital Payment Systems—](#) ► [kuleuven.ac.be](#)

[PDF]
 JP Boly, A Bosselaers, R Cramer, R Michelsen, S ... - Computer Security-ESORICS 94: Third European
 Symposium on ..., 1994 - books.google.com
 ... A Method for Obtaining Digital Signatures and **Public- Key** Cryptosystems; Communications
 of ... Waid 94 Michael Waidner: CAFE-**Conditional Access** for Europe; 4. GMD ...
[Cited by 118](#) - [Related articles](#) - [Web Search](#) - [BL Direct](#) - [All 26 versions](#)

[An overview of multimedia content protection in consumer electronics devices-](#) ► [cuny.edu](#)

[PDF]
 AM Eskicioglu, EJ Delp - Signal Processing: Image Communication, 2001 - Elsevier
 ... Both symmetric and **public key** ciphers are commonly used for content ... Such architectures
 are considered extensions of **conditional access** systems, restricting ...

[Cited by 104](#) - [Related articles](#) - [Web Search](#) - [All 23 versions](#)

Development of a secure electronic marketplace for Europe- ► [psu.edu](#) (pdf)

M Waidner - LECTURE NOTES IN COMPUTER SCIENCE, 1996 - Springer

... might receive a specific certificate that subsequently enables **conditional access** to certain ... They all require a **public-key** infrastructure Both SSL and SHITP ...

[Cited by 44](#) - [Related articles](#) - [Web Search](#) - [BL Direct](#) - [All 16 versions](#)

Model-based verification of a security protocol for **conditional access** to services- ► [psu.edu](#)

(PDF)

G Leduc, O Bonaventure, L Leonard, E Koerner, C ... - Formal Methods in System Design, 1999 - Springer

... with proprietary systems which all use different **conditional access** protocols and ... service (provider), a unique decoder uses a **public-key** cryptography protocol ...

[Cited by 9](#) - [Related articles](#) - [Web Search](#) - [BL Direct](#) - [All 6 versions](#)

Advances in **conditional access** technology

W Mooij, I Consultants - Broadcasting Convention, 1997. International, 1997 - [ieeexplore.ieee.org](#)

... are based on DES-like schemes often in combination with **public key** based components ...

This allows modern **Conditional Access** systems a great deal of flexibility to ...

[Cited by 7](#) - [Related articles](#) - [Web Search](#) - [BL Direct](#) - [All 4 versions](#)

Some general methods for tampering with watermarks- ► [ucla.edu](#) (pdf)

IJ Cox, JPMG Linnartz - IEEE Journal on selected areas in communications, 1998 - [ieeexplore.ieee.org](#)

... In the past [8], we have described such systems as "public" watermarks, drawing analogy with **public key** cryptography. However, this is misleading. ...

[Cited by 232](#) - [Related articles](#) - [Web Search](#) - [BL Direct](#) - [All 29 versions](#)

(PDF) ► A Key Transport Protocol Based on Secret Sharing—An Application to **Conditional Access Systems**

AM Eskicioglu, T Multimedia - IS&T/SPIE's 13 th International Symposium on Electronic ..., 2001 - Citeseer

... Key words: **conditional access**, content protection, key transport, multimedia, **public-key** cryptography, secret sharing, symmetric cipher. 1. INTRODUCTION ...

[Cited by 4](#) - [Related articles](#) - [View as HTML](#) - [Web Search](#) - [All 9 versions](#)

Apparatus and method for providing secured communications

DL Davis - US Patent 5,805,712, 1998 - Google Patents

... Guillou, L.: "Smart Cards and **Conditional Access**" in Advances in Cryptology—Proceedings of EUROCRYPT 84; T Beth, N ... Output **public key** to g certification s stem ...

[Cited by 48](#) - [Related articles](#) - [Web Search](#) - [All 6 versions](#)

Networked workstation intrusion detection system

J Trostle - US Patent 5,919,257, 1999 - Google Patents

... pre-boot modules, a root master **public key** (ie, the **public key** associated with ... onto the network and the workstation user is granted **conditional access** to the ...

[Cited by 35](#) - [Related articles](#) - [Web Search](#) - [All 2 versions](#)

Verification of the source of program information in a **conditional access** system

HG Pinder, MS Paigon, GL Akins III, RO Banker - US Patent 6,105,134, 2000 - Google Patents

... A. Gardner [57] ABSTRACT A cable television system provides **conditional access** to services ... PIN EA **PUBLIC KEY** EAD \i ^HEADER -1502 hCAA FIELDS 1506 \- EA FIELDS ...

[Cited by 11](#) - [Related articles](#) - [Web Search](#) - [All 2 versions](#)

Dynamic traitor tracing- ► [saitama-u.ac.jp](#) (pdf)

A Fiat, T Tassa - Journal of Cryptology, 2001 - Springer

... In such systems the content is distributed via terrestrial, cable, or satellite broadcast and, hence, a **conditional access** system must be utilized in order to ...

[Cited by 121](#) - [Related articles](#) - [Web Search](#) - [BL Direct](#) - [All 20 versions](#)

Scrambling and key distribution scheme for digital television

W Kanjanarin, T Amornraksa - Ninth IEEE International Conference on Networks, 2001. ..., 2001 - [ieeexplore.ieee.org](#)

... kmut t . ac . th Abstract The scrambling scheme is a part of the **conditional access** system (CAS) that is used to prevent unauthorized access to Pay-TV systems. ...

[Cited by 13](#) - [Related articles](#) - [Web Search](#) - [All 3 versions](#)

[PDF] ► Digital transmission content protection

B Pearson - Jun, 1999 - [dtcp.com](#)

... Page 19. © 19 Full Authentication (**public key** cryptography) – Supports all types of content ... 21 DTCP Example **Conditional Access** System Internet Cable Provider ...

[Cited by 5](#) - [Related articles](#) - [View as HTML](#) - [Web Search](#)

Evaluation of different video encryption methods for a secure multimedia conferencing gateway- ► [tu-darmstadt.de](#) [PDF]

T Kunkelmann, T Blecher, R Reinema, R Steinmetz - Lecture notes in computer science, 1997 - Springer

... 77 • **Public Key** Encryption (eg RSA and Diffie-HeUman) • Hybrid Encryption ... 82 4.7

DVB - **Conditional Access Conditional Access** (CA) is a method for video ...

[Cited by 16](#) - [Related articles](#) - [Web Search](#) - [BL Direct](#) - [All 5 versions](#)

Nark: Receiver-based multicast non-repudiation and key management- ► [psu.edu](#) [PDF]

B Briscoe, I Fairman - Proceedings of the 1st ACM conference on Electronic commerce, 1999 - [portal.acm.org](#)

... If receivers require each sender to authenticate their messages individually, **public key** signing leads to an unscalable solution because of the sheer volume of ...

[Cited by 25](#) - [Related articles](#) - [Web Search](#) - [All 10 versions](#)

Conditional access and content security method

RR Sullivan, JM Acken, DW Aucsmith - US Patent 6,069,647, 2000 - Google Patents

... Date of Patent: 6,069,647 May 30,2000 [54] **CONDITIONAL ACCESS AND CONTENT ... DIGITAL CERTIFICATE FROM PROGRAMMABLE UNIT TO OBTAIN ITS PUBLIC KEY (PUKPU) ENCRYPT ...**

[Cited by 4](#) - [Related articles](#) - [Web Search](#) - [All 2 versions](#)

Novel applications of cryptography in digital communications

JK Omura - IEEE Communications Magazine, 1990 - [ieeexplore.ieee.org](#)

... IN 1976, DIFFIE AND HELLMAN [1] STARTED AN explosion of open research in cryptology when they introduced the notion of **public-key** cryptography [2]. Today there ...

[Cited by 24](#) - [Related articles](#) - [Web Search](#) - [All 3 versions](#)

Beyond cryptographic **conditional access**

DM Goldschlag, DW Kravitz - Proceedings of the USENIX Workshop on Smartcard Technology ..., 1999 - [portal.acm.org](#)

... 3. Non-Cryptographic **Conditional Access** ... device may issue a randomly generated bit-string, where the concatenation of this bit-string with the **public key** of a ...

[Cited by 4](#) - [Related articles](#) - [Web Search](#) - [All 3 versions](#)

Model-based design and verification of security protocols using LOTOS- ► [kfupm.edu.sa](#) [PDF]

F Germeau, G Leduc - Rutgers University, 1997 - [eprints.kfupm.edu.sa](#)

... Thus we will focus on two examples that represent the most widely used operations: encryption and signature in **public-key** cryptography. ...

[Cited by 18](#) - [Related articles](#) - [View as HTML](#) - [Web Search](#) - [All 5 versions](#)

Cryptographic authentication protocols for smart cards

LC Guillou, M Ugon, JJ Quisquater - Computer Networks, 2001 - Elsevier
 ... of **public key** features. This is not surprising because integer factorization and silicon investigation are both complex problems. 2.7. **Conditional access** to ...
 Cited by 11 - Related articles - Web Search - All 3 versions

The smart card: don't leave home without it

D Husemann - IEEE concurrency, 1999 - ieeexplore.ieee.org
 ... from **conditional access** methods for satel- lite TV to electronic signature applications ...
 stored on the card, we can also implement **public key** signature schemes ...
 Cited by 14 - Related articles - Web Search - All 6 versions

A prepositioned secret sharing scheme for message authentication in broadcast networks-

► [cuny.edu](#) [PDF]
 AM Eskicioglu - Proceedings of the Communications and Multimedia Security ..., 2001 - books.google.com
 ... Authority (CA) who creates, distributes, maintains and revokes **public-key** certificates ...
 proposed for protecting audio/video content in **conditional access** systems4 ...
 Cited by 6 - Related articles - Web Search - All 7 versions

Management of a **public key** certification infrastructure—experiences from the DeTeBerkom project ...

M Gehrke, T Hetschold - Computer Networks and ISDN Systems, 1996 - Elsevier
 ... Keywords: **Public key** certification; Certification authority; Personal secure environment; X.700 management ... able without a strong **conditional access** scheme [11 ...
 Cited by 5 - Related articles - Web Search - BL Direct - All 4 versions

On the design of conference key distribution systems for the broadcasting networks

CS Laih, SM Yen - INFOCOM, 1993 - citeseer.ist.psu.edu
 ... on text: More All 0.6: On Key Distribution Management For - **Conditional Access** System
 (Correct ... 1529 A Method for Obtaining Digital Signatures and **Public--Key** Cr ...
 Cited by 7 - Related articles - Cached - Web Search - BL Direct - All 2 versions

Conditional access system

AJ Wasilewski, HG Pinder, GL Akins, MS Palgon - US Patent App. 09/881,428, 2001 - Google Patents
 ... 239; 725/31 (57) ABSTRACT A cable television system provides **conditional access** to services. ... 1502 -CAA FIELDS -1506 > EA FIELDS 1516 FIG-15 EA **PUBLIC KEY** EAD u ...
 Cited by 5 - Related articles - Web Search - All 4 versions

Public-key techniques: randomness and redundancy

LC Guillou, M Davio, JJ Quisquater - Cryptologia, 1989 - informaworld.com
 Guillou, Davio, and Quisquater **Public-Key** Techniques: Randomness and Redundancy
PUBLIC-KEY TECHNIQUES: RANDOMNESS AND REDUNDANCY Louis C. Guillou W, Marc Davio ...
 Cited by 11 - Related articles - Web Search

[PDF] ► Secure mediation: Requirements and design

J Biskup, U Flegel, Y Karabulut - DATABASE SECURITY, 1999 - Citeseer
 ... otherwise. For the basic protocols we always only need the **public key** for encryption in credentials, as sketched in the following. ...
 Cited by 23 - Related articles - View as HTML - Web Search - BL Direct - All 8 versions

[PDF] ► A computer aided design of a secure registration protocol

F Germeau, G Leduc - Formal Description Techniques and Protocol Specification, ..., 1997 - eprints.kfupm.edu.sa
 ... 1996) is a **conditional access** protocol under design in the European ACTS OKAPI ...
 successful registra- tion, this third party issues a **public-key** certicate which ...

[Cited by 8](#) - [Related articles](#) - [View as HTML](#) - [Web Search](#) - [All 12 versions](#)

Broadcast encryption- [psu.edu](#) [pdf](#)

A Fiat - US Patent 5,592,552, 1997 - Google Patents

... Rivest, RL, et al., A method for obtaining digital signature and **public-key** cryptosystems, Communications of the ACM, V 21, N 2, Feb. 1978, pp. 120-126. ...

[Cited by 610](#) - [Related articles](#) - [Web Search](#) - [BL Direct](#) - [All 14 versions](#)

Securing the AES finalists against power analysis attacks

TS Messerges - Lecture notes in computer science, 2001 - Springer

... 99 [14]. Researchers have also begun to study the vulnerabilities of **public-key** cryptosystems to these attacks [23, 24]. Power analysis ...

[Cited by 125](#) - [Related articles](#) - [Web Search](#) - [BL Direct](#) - [All 5 versions](#)

[\[PDF\] Secure delivery of images over open networks](#)

D Augot, JM Boucqueau, JF Delaigle, C Fontaine, E ... - Proceedings of the IEEE, 1999 - www-rocq.inria.fr

... delivery systems in which watermarking, monitoring, and **public key** infrastructures based ... C. **Conditional Access** Systems (CAS's) Access control is the denial ...

[Cited by 29](#) - [Related articles](#) - [View as HTML](#) - [Web Search](#) - [BL Direct](#) - [All 10 versions](#)

Verification of security protocols using LOTOS-method and application- [ulg.ac.be](#) [pdf](#)

G Leduc, F Germeau - Computer Communications, 2000 - Elsevier

... Thus we will focus on two examples that represent the most widely used operations: encryption and signature in **public-key** crypto- graphy. ...

[Cited by 31](#) - [Related articles](#) - [Web Search](#) - [All 10 versions](#)

[\[PDF\] Analysis of privacy and non-repudiation on pay-TV systems](#)

R Song, MR Lyu - IEEE Transactions on Consumer Electronics, 2001 - cse.cuhk.edu.hk

... A mechanism called a **Conditional Access** System (CAS) is employed on Pay-TV systems to ... X_K : user LPs secret key • PKV: user If s **public key** • K_s 'a ...

[Cited by 6](#) - [Related articles](#) - [Web Search](#) - [BL Direct](#) - [All 9 versions](#)

Public-key cryptography on smart cards

A Fuchsberger, D Gollmann, P Lothian, KG Paterson, ... - Lecture Notes in Computer Science, 1996 - Springer

Page 1. **Public-key** Cryptography on Smart Cards ... **Public key** cryptosystems on smart cards are thus a very attractive proposition for this kind of applications. ...

[Cited by 4](#) - [Related articles](#) - [Web Search](#) - [BL Direct](#) - [All 2 versions](#)

MARKS: Zero side effect multicast key management using arbitrarily revealed key sequences-

[ucl.ac.uk](#) [pdf](#)

B Briscoe - Lecture Notes in Computer Science, 1999 - Springer

... way to do this is for all S and KM to run secure Web servers so that the session key can be sent to each of them encrypted with each **public key** using client ...

[Cited by 109](#) - [Related articles](#) - [Web Search](#) - [BL Direct](#) - [All 15 versions](#)

Pirate Card Rejection

DM Goldschlag, DW Kravitz - Lecture notes in computer science, 2000 - Springer

... that the renewable device does content decryption in addition to **conditional access**

(Fig ... which pairs the particular host with a particular card's **public key**. ...

[Cited by 4](#) - [Related articles](#) - [Web Search](#) - [BL Direct](#) - [All 4 versions](#)

The DVB multimedia home platform-" MHP

J Piesing - IEE Colloquium on Interactive Television (Ref. No. 1999/200), 1999 - ieeeexplore.ieee.org

... defined for the transmission of digital signatures for applications and to

connect those to conventional **public key** certificates. When ...

[Cited by 8](#) - [Related articles](#) - [Web Search](#) - [BL Direct](#)

Towards secure mediation

J Biskup, U Flegel, Y Karabulut - Workshop Sicherheit und Electronic Commerce, Essen, Germany, 1998 - Is6-
www.informatik.uni-dortmund.de

... as plaintext and encrypted with (some of) the **public key(s)** occurring in ... **Conditional Access** Workshop, 44th RACE Concertation Meeting , Brussel, November 1994. ...

[Cited by 10](#) - [Related articles](#) - [View as HTML](#) - [Web Search](#) - [All 6 versions](#)

Fully meshed CDMA network for personal communications terminals

RJ Fang - US Patent 5,481,561, 1996 - Google Patents

Page 1. United States Patent Fang US005481561A [ii] Patent Number: [45]

Date of Patent: 5,481,561 Jan. 2, 1996 [54] FULLY MESHED ...

[Cited by 10](#) - [Related articles](#) - [Web Search](#) - [All 7 versions](#)

See what you sign: Secure implementations of digital signatures- [► psu.edu \(pdf\)](#)

A Weber - Lecture notes in computer science, 1998 - Springer

... A message bearing a digital signature verified by the **public key** listed in a ... 7023

CAFE (**Conditional Access** for Europe) of the European Union, 1992-1996 7 It is ...

[Cited by 15](#) - [Related articles](#) - [Web Search](#) - [BL Direct](#) - [All 9 versions](#)

Personal and thin-route communications via K-bandsatellite transponders

RJF Fang - IEEE Military Communications Conference, 1991. MILCOM'91, ..., 1991 - ieeexplore.ieee.org

... Communications privacy and **conditional access** canbe incorporated
intothePCTbyusingencryption. ... On the other hand, if a **public key** encryption ...

[Cited by 4](#) - [Related articles](#) - [Web Search](#) - [All 3 versions](#)

Issues for the Commercial Distribution of Electronic Documents- [► psu.edu \(pdf\)](#)

V Prevelakis, D Konstantas, JH Morin - Communications and Multimedia Security, 1997 - books.google.com

... is unique for each transaction, is then encrypted using RSA **public key** technology ...

CAFE [1 7](**Conditional Access** For Europe) is an ESPRIT project that developed ...

[Cited by 13](#) - [Related articles](#) - [Web Search](#) - [All 6 versions](#)

Source authentication of download information in a **conditional access** system

GL Akins, RO Banker, MS Palgon, HG Pinder, AJ ... - US Patent App. 09/748,313, 2000 - Google Patents

... 380/241; 380/239; 380/229 (57) ABSTRACT A cable television system provides **conditional access** to services ... 15H 1525-J PIN J FIG 15 1527-^ EA **PUBLIC KEY** -1506 JJ ...

[Cited by 2](#) - [Related articles](#) - [Web Search](#) - [All 8 versions](#)

Representing entitlements to service in a **conditional access** system

GL Akins, RO Banker, MS Palgon, HG Pinder, AJ ... - US Patent App. 09/930,901, 2001 - Google Patents

... CI 380/282 (57) ABSTRACT A cable television system provides **conditional access** to services. ... PIN EA **PUBLIC KEY** EAD 14 -HEADER -1502 •CAA FIELDS 1506 EA FIELDS ...

[Cited by 2](#) - [Related articles](#) - [Web Search](#) - [All 8 versions](#)

[PDF] [► Digital rights management for digital cinema](#)

D Kirovski, M Peinado, FAP Petitcolas - invited paper in Security in Imaging: Theory and ..., 2001 - Citeseer

... The general goal is to ensure secure distribution of the content and enforce **conditional access** to it. ... We base authentication on **public-key** cryptography. ...

[Cited by 8](#) - [Related articles](#) - [View as HTML](#) - [Web Search](#) - [All 14 versions](#)

System and method for providing security in data communication systems

BK Ichikawa - US Patent 5,872,846, 1999 - Google Patents

... permission, or the **Conditional Access** method, and is ... this instance, the key that

is used to encrypt the data is designated as a receiver's **public key**, in that ...

[Cited by 2](#) - [Related articles](#) - [Web Search](#) - [All 6 versions](#)

[\[PDF\] ► Copy protection for DVD video](#)

JA Bloom, IJ Cox, T Kalker, JPMG Linnartz, ML ... - Proceedings of the IEEE, 1999 - Citeseer
... Exchange using a 160-bit elliptic curve **public key** cryptosystem compat ... interconnects
including the Universal Serial Bus, **conditional access** smartcard interfaces ...

[Cited by 171](#) - [Related articles](#) - [View as HTML](#) - [Web Search](#) - [BL Direct](#) - [All 31 versions](#)

[\[PDF\] ► Implementing protocol verification for E-commerce](#)

B Aziz, D Gray, G Hamilton, F Oehl, J Power, D ... - Proceedings of the 2001 International Conference on
Advances ..., 2001 - antareja.rvs.uni-bielefeld.de

... Providing Equitable **Conditional Access** by Use of Trusted Third Parties. ... G. Lowe.
Breaking and Fixing the Needham-Schroeder **Public-Key** Protocol Using FDR. ...

[Cited by 4](#) - [Related articles](#) - [View as HTML](#) - [Web Search](#) - [All 2 versions](#)

[Towards a mechanization of cryptographic protocol verification](#)

D Bolignano - Lecture Notes in Computer Science, 1997 - Springer

... by a particular principal and is known as the private key of this principal, whereas
the other one is not confidential and is known as the **public key** of this ...

[Cited by 64](#) - [Related articles](#) - [Web Search](#) - [BL Direct](#) - [All 4 versions](#)

[Secured Web access- ► purdue.edu \[pdf\]](#)

M Mohania, V Kumar, Y Kambayashi, B Bhargava - Digital Libraries: Research and Practice, 2000 Kyoto, ...,
2000 - ieeeexplore.ieee.org

... is verified, the user is either given **conditional access**, timed access ... **Public key**
cryptographic systems provide a more sophisticated form of authentication that ...

[Cited by 3](#) - [Related articles](#) - [Web Search](#) - [All 3 versions](#)

[\[PS\] ► A security platform for future telecommunication applications and services](#)

M Gehrke, E Koch - Proc. of the 6th Joint European Networking Conference, 1992 - igd.fhg.de

... Information with low variation frequency, such as **public key** certificates, will
be stored ... Proceedings of the RACE Workshop on **Conditional Access**, Bruessel, Nov ...

[Cited by 5](#) - [Related articles](#) - [View as HTML](#) - [Web Search](#) - [All 3 versions](#)

[Method of electronic payment by chip card by means of numbered tokens allowing the detection of ...](#)

LC Guillou, JJ Quisquater - US Patent 5,305,383, 1994 - Google Patents

... For **conditional access**, keyholder cards are used ... the keys used for managing the elements
of the system 15 which is beyond his control **Public-key** algorithms will ...

[Cited by 10](#) - [Related articles](#) - [Web Search](#) - [All 2 versions](#)

[A simple micro-payment scheme](#)

MS Hwang, IC Lin, LH Li - The Journal of Systems & Software, 2001 - Elsevier

... This protocol uses **public-key** cryptography and applies CA-based security. ... Page
3. and **Conditional Access** for Europe (CAFE) (Boly et al., 1994). ...

[Cited by 37](#) - [Related articles](#) - [Web Search](#) - [All 4 versions](#)

[Document management system](#)

M Hajmiragha - US Patent 6,289,460, 2001 - Google Patents

... 98 provides 55 to users to publish a user's **public key** to verify ... man- ager 104 includes
process flow templates that generate **conditional Access** Control List ...

[Cited by 3](#) - [Related articles](#) - [Web Search](#) - [All 7 versions](#)

Data security issues, cryptographic protection methods, and the use of cellular neural networks and ...

J Vandewalle, B Preneel, M Csapodi - Cellular Neural Networks and Their Applications Proceedings, ..., 1998 - ieeexplore.ieee.org

... Existing implementations of **conditional access** systems (eg, Canal+ pay-TV service) use ... However the **public-key** algorithms are much more difficult to design. In ...

[Cited by 3](#) - [Related articles](#) - [Web Search](#)

[PDF] ► Yet Another Simple Internet Electronic Payment System

J Zhao, C Dong, E Koch - Proc. of the IFIP 1996 World Conference-Mobile ..., 1996 - Citeseer

... designer W. Mao, the system does not utilize **public key** certification infrastructure ... CAFE (**Conditional Access** for Europe) is a project in the European Community ...

[Cited by 2](#) - [Related articles](#) - [View as HTML](#) - [Web Search](#) - [All 6 versions](#)

A new method of Internet access within a DBS environment

JH Hahn, DH Han, KH Lee, JC Ryou, TT Div, T ETRI - IEEE Transactions on Consumer Electronics, 1998 - ieeexplore.ieee.org

... The **conditional access** services prevent programs or data from being accessed by unauthorized users but it is only available for ... **public key** mechanism are used. ...

[Cited by 1](#) - [Related articles](#) - [Web Search](#) - [BL Direct](#) - [All 2 versions](#)

Keeping card data secure at low cost

AW Vaidya, TSS Int - Security and Detection, 1995., European Convention on, 1995 - ieeexplore.ieee.org

... can have in addition to memory some logic circuitry giving **conditional access** and a ... recovered from the memory and decrypted using the appropriate **public key**. ...

[Cited by 2](#) - [Related articles](#) - [Web Search](#) - [BL Direct](#) - [All 2 versions](#)

Programmable telecommunications security module for key encryption adaptable for tokenless use

PA Walter, EP McGrogan Jr, M Kleidermacher - US Patent 6,151,677, 2000 - Google Patents

... The security of both single-key and **public-key** encryption systems depends on ... an integrated circuit (1C) chip 130 designed for **conditional access** systems which ...

[Cited by 2](#) - [Related articles](#) - [Web Search](#) - [All 6 versions](#)

An Integrated Secure Web Architecture For Protected Mobile Code Distribution- ► fhg.de [PDF]

M Jalali-Sohi, R Foka, G Hachez, A Beitlich - Communications and Multimedia Security Issues of the New ..., 2001 - books.google.com

... for Jar files recommended by inventors of the RSA **public-key** cryptography and ... OCTALIS [8] This project studied how to couple **conditional access** and copyright ...

[Cited by 2](#) - [Related articles](#) - [Web Search](#) - [All 8 versions](#)

[PDF] ► Security protocols over open networks and distributed systems: Formal methods for their analysis, ...

S Gritzalis, D Spinellis, P Georgiadis - Computer Communications, 1999 - eprints.kfupm.edu.sa

... used to model the Equicrypt protocol [38] for **conditional access** to multimedia serv ... has been applied on the Needham-Schroeder **public-key** authentication protocol ...

[Cited by 86](#) - [Related articles](#) - [View as HTML](#) - [Web Search](#) - [All 12 versions](#)

Process for protecting an information item transmitted from a security element to a decoder and ...

A Campinos, JB Fischer - US Patent 6,266,415, 2001 - Google Patents

... the said data representing at least one programme selected by a **conditional-access** system user. ... 2, a **public key** algorithm can be used for the devices 9 and 10. ...

[Cited by 1](#) - [Related articles](#) - [Web Search](#) - [All 4 versions](#)

Firewalling the net

SD Hubbard, JC Sager - BT Technology Journal, 1997 - Springer

Page 1. BT Technol J Vol 15 No 2 April 1997 94 Firewalling the Net SD Hubbard and JC Sager To connect any stand-alone enterprise ...

[Cited by 17](#) - [Related articles](#) - [Web Search](#) - [All 5 versions](#)

Authorization and access control of software object residing in set-top terminals

R Safadi, L Vince - US Patent 6,256,393, 2001 - Google Patents

... the utilization of a set-top resource, a second **conditional access** routine may be ... which is not published) and is verified with Microsoft's **public key**, which is ...

[Cited by 2](#) - [Related articles](#) - [Web Search](#) - [All 6 versions](#)

System for controlling access to a function having clock synchronization

Y Audebert - US Patent 5,737,421, 1998 - Google Patents

... condition is not satisfied, 65 The system is assumed to grant **conditional access** to a ... mode" device in which 55 algorithm itself may use a **public key** or a ...

[Cited by 4](#) - [Related articles](#) - [Web Search](#) - [All 3 versions](#)

Method and apparatus for controlling the operation of a signal decoder in a broadcasting system

M von Willich, SPA Rix - US Patent 6,021,197, 2000 - Google Patents

... Enhanced Cost effective Line Shuffle Scrambling System with Secure **Conditional Access** Autho- rization ... decrypt signature using **public key** transport stream on list ...

[Cited by 1](#) - [Related articles](#) - [Web Search](#) - [All 5 versions](#)

Key management for encrypted broadcast- ►[lau.ac.il](#) [PDF]

A Wool - ACM Transactions on Information and System Security (TISSEC), 2000 - portal.acm.org

... General Terms: Security Additional Key Words and Phrases: **Conditional access**, pay-per ... However, their techniques rely on RSA **public-key** cryptography [Rivest et ...

[Cited by 26](#) - [Related articles](#) - [Web Search](#) - [All 14 versions](#)

Personal communications via INTELSAT K u-band transponders

RJF Fang - International Journal of Satellite Communications, 1992 - interscience.wiley.com

... Communications privacy and **conditional access** can be incorporated into the PCT by using ... On the other hand, if a **public key** encryption system is employed for ...

[Cited by 1](#) - [Related articles](#) - [Web Search](#) - [BL Direct](#) - [All 5 versions](#)

[PDF] ► Multimedia watermarking techniques

F Hartung, M Kutter - Proceedings of the IEEE, 1999 - vis.uky.edu

... is a key requirement for copy- right protection or **conditional access** applications, but ... can, for example, embed two watermarks, one with a **public key** and the ...

[Cited by 759](#) - [Related articles](#) - [View as HTML](#) - [Web Search](#) - [BL Direct](#) - [All 18 versions](#)

System and method for user authentication having clock synchronization

Y Audebert - US Patent 5,887,065, 1999 - Google Patents

... second unit. The second unit grants **conditional access** to a lunction or service in accordance with an authentication operation. Both ...

[Cited by 8](#) - [Related articles](#) - [Web Search](#) - [All 2 versions](#)

Supplemental **conditional access** for DSS

R Takahashi, J Wallace - Consumer Electronics, 1996. Digest of Technical Papers., ..., 1996 - ieeexplore.ieee.org

... Implementation and Architecture The supplemental DSS **conditional access** is based on the **public key** concept to distribute content keys and provide ...

[Web Search](#) - [BL Direct](#) - [All 2 versions](#)

CONDITIONAL ACCESS SYSTEM FOR DIGITAL RECEIVERS

A ESKICIOGLU, M OZKAN, B BEYERS Jr - 1999 - freepatentsonline.com

... **Conditional Access** Organization (CA) 75 is not directly connected to either the ... sharing which eliminates the requirement for using **public key** cryptography to ...

[Related articles](#) - [Web Search](#) - [All 5 versions](#)

Smartcard uart for minimizing processor demands in a **conditional access** system

DJ Duffield, JA Cooper, M Narasimhan - US Patent App. 10/490,679, 2001 - Google Patents

... is preferably used in a smart card of a **conditional access** system, it ... 21, 2005 **public key** infrastructure (PKI) key management systems, video game systems, etc ...

[Web Search](#) - [All 6 versions](#)

Method and apparatus for controlling the operation of a signal decoder in a broadcasting system

WM Von, RSP Ashley - EP Patent 0.750.423, 1996 - freepatentsonline.com

... **conditional access** module 13 includes a descrambler 17 with **conditional access** data filters ... then encrypted using a secret key of a **public key** encryption method ...

[Web Search](#) - [All 2 versions](#)

[PDF] ► On the Security of Digital Video Distribution Systems

A Adas, T Tran, AN Tantawy - 1996 - Citeseer

... provide high speed encryption of exchanged data, while **public key** systems are used for secure and ... 3 An Example Broadcast System with **Conditional Access** ...

[Related articles](#) - [View as HTML](#) - [Web Search](#) - [Library Search](#) - [All 2 versions](#)

A COPY PROTECTION SYSTEM FOR HOME NETWORKS

A ESKICIOGLU, W BEYERS Jr, P It - 2000 - freepatentsonline.com

... provider sends a **conditional access** (CA) entitlement message (ie, an Entitlement Control Message or ECM) in the bit stream encrypted by the **public key** that may ...

[Web Search](#) - [All 5 versions](#)

Systems and devices for the cryptography of digital signals.

S Cucchi, G Parladori, R Maestri, P It - 1992 - freepatentsonline.com

... 8 June 1985, MONTREUX (CH) pages 186 - 194; SM EDWARDSON: 'A **Conditional Access** System for ... according to claim 1, in which it is used the **public key** technics to ...

[Web Search](#) - [All 3 versions](#)

ENCRYPTION DEVICES FOR USE IN A **CONDITIONAL ACCESS** SYSTEM

M PALGON, H PINDER - 1999 - freepatentsonline.com

... 1. If the service is provided by an entitlement agent for which the customer's DHCT 333 does not have the **public key**, the **conditional access** authority must ...

[Related articles](#) - [Web Search](#) - [All 5 versions](#)

A GLOBAL COPY PROTECTION SYSTEM FOR DIGITAL HOME NETWORKS

A ESKICIOGLU, D VIRAG, D DUFFIELD, M DEISS, B ... - 2000 - freepatentsonline.com

... 6. The method of Claim 5 wherein the step of initializing comprises the step of receiving a **public key** from a **conditional access** provider, said step of ...

[Web Search](#) - [All 5 versions](#)

Remote e-purse payment system

C Genevois, W Neifer, M Krall - US Patent App. 09/936,303, 2001 - Google Patents

... but open architecture to allow interaction of diverse **conditional access** systems with one ... to a specific provider) [0038] 2bb) filters a **public-key** for reading ...

[Web Search](#) - [All 6 versions](#)

A Trusted Third Party Network for the Equi© rypt Access Control System

AFA Teledetection - Global Information Infrastructure (GII) Evolution: ..., 1996 - books.google.com

... minimal set of functionality allowing a customized open **conditional access** system

implementation ... will be detailed in Section 3; c) **Public Key** cryptography: will ...

[Related articles](#) - [Web Search](#)

Descrambling device for use in a **conditional access** system

KC Bacon - US Patent App. 09/780,544, 2001 - Google Patents

... Date: Aug. 15, 2002 (54) DESCRAMBLING DEVICE FOR USE IN A **CONDITIONAL ACCESS** SYSTEM

(76) Inventor: Kinney C. Bacon, Lawrenceville, GA (US) Correspondence Address ...

[Web Search](#) - [All 6 versions](#)

VERIFICATION OF THE SOURCE OF PROGRAM OF INFORMATION IN A **CONDITIONAL ACCESS** SYSTEM

GL Akins III, RO Banker, MS Palgon, HG Pinder - EP Patent 1,010,323, 2001 - freepatentsonline.com

... 1. If the service is provided by an entitlement agent for which the customer's DHCT

333 does not have the **public key**, the **conditional access** authority must ...

[Related articles](#) - [Web Search](#) - [All 5 versions](#)

CA system for broadcast DTV using multiple keys for different service providers and service areas

A Eskicioglu, DJ Duffield, BW Beyers, MS Deiss, DE ... - US Patent App. 09/962,970, 2001 - Google Patents

... service providers. [0012] Such a **conditional access** system as the one described

above may be based on **public key** technology. At least ...

[Web Search](#) - [All 6 versions](#)

AUTHORIZATION OF SERVICES IN A **CONDITIONAL ACCESS** SYSTEM

GL Akins III, RO Banker, HG Pinder, AJ Wasilewski - EP Patent 1,000,508, 2001 - freepatentsonline.com

... 1. If the service is provided by an entitlement agent for which the customer's DHCT

333 does not have the **public key**, the **conditional access** authority must ...

[Web Search](#) - [All 6 versions](#)

Method, encoding apparatus and decoding apparatus for protecting a data stream using encryption or ...

K Gaedke, H Peters, H Schutze - US Patent App. 09/780,727, 2001 - Google Patents

... digital transmission content protection) or XCA (extended **conditional access**) exist ...

encryption mentioned above is generated using a **public key** encryption system ...

[Web Search](#) - [All 5 versions](#)

CONDITIONAL ACCESS SYSTEM

GL Akins III, MS Palgon, HG Pinder, AJ Wasilewski - EP Patent 1,000,511, 2001 - freepatentsonline.com

... 1. If the service is provided by an entitlement agent for which the customer's DHCT

333 does not have the **public key**, the **conditional access** authority must ...

[Related articles](#) - [Web Search](#) - [All 5 versions](#)

Method and apparatus for generating a data stream protected by encryption

K Gaedke, H Peters, H Schuetze - EP Patent 1,124,376, 2001 - freepatentsonline.com

... For PKES and PKDS a well-known **public key** encryption algorithm like eg RSA ... Further, the encryption of the VLC code tables also allows **conditional access** to the ...

[Web Search](#) - [All 4 versions](#)

An embedded cryptosystem for digital broadcasting

GS Sundaram, S Sista - 1997 IEEE 6th International Conference on Universal Personal ..., 1997 - [ieeexplore.ieee.org](#)

... Digital multimedia broadcasting, needs new cryptographic tools for **conditional access**. ... problems can be avoided by using a **public key** encryption scheme ...

[Related articles](#) - [Web Search](#)

[System for securing encryption renewal system and for registration and remote activation of ...](#)

Jl Okimoto, LW Tang - US Patent App. 09/898,168, 2001 - Google Patents

... information about which video on demand system is associated with the **conditional access** system ... or more of a secret shared key, a private key, and a **public key**. ...

[Web Search](#) - [All 5 versions](#)

[Content packet distribution system](#)

RW Schumann, R Whittemore, DM Goldschlag, DW ... - US Patent App. 09/880,855, 2001 - Google Patents

... The system proposed by Peterson uses a **public key** held at an authorization center ... protection architecture that may be used to provide **conditional access** to data ...

[Web Search](#) - [All 4 versions](#)

[Secure time reference for content players](#)

BL Candelore - US Patent App. 09/854,021, 2001 - Google Patents

... in decrypted format, 130, to the content player and **Conditional Access** module as ... consumer's content player in this embodiment, uses the **public key** to encrypt a ...

[Web Search](#) - [All 2 versions](#)

[METHOD AND APPARATUS FOR USE OF A WATERMARK AND A RECEIVER
DEPENDENT REFERENCE FOR THE PURPOSE OF ...](#)

MA EPSTEIN - US Patent App. 09/320,806, 1999 - Google Patents

... utilized as a unique receiver identifier and a private/ **public key** system is ... another embodiment, the source device 230 may be a **conditional access** (CA) device. ...

[Web Search](#) - [All 6 versions](#)

[System and method for authenticating the location of content players](#)

BL Candelore - US Patent App. 09/840,226, 2001 - Google Patents

... 2 may comprise a Point of Deployment (POD) **conditional access** module, a ... cryptographic CPU 230 securely communicates using secret or **public key** cryptography ...

[Web Search](#) - [All 2 versions](#)


[Scrambling unit for a digital transmission system](#)

L Tranchard, C Declerck, P It - 1999 - freepatentsonline.com

... arrangement is used, the scrambling unit possesses an equivalent **public key** permitting the ... control word generator 3 and one or more **conditional access** systems 6 ...

[Related articles](#) - [Web Search](#) - [All 6 versions](#)

Key authors: [M Waidner](#) - [L Guillou](#) - [A Fiat](#) - [I Cox](#) - [F Hartung](#)

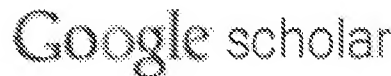
Google 

Result Page: 1 2 [Next](#)

"public key" "conditional access"

[Go to Google Home](#) - [About Google](#) - [About Google Scholar](#)

[Web](#)
[Images](#)
[Video](#)
[News](#)
[Maps](#)
[more »](#)



☒ Search only in Engineering, Computer Science, and Mathematics.
 ☐ Search in all subject areas.

Scholar All articles - **Recent articles** Results 1 - 47 of 47 for "public key" "conditional access" hie

Cryptology for digital TV broadcasting

BM Macq, JJ Quisquater - Proceedings of the IEEE, 1995 - ieeexplore.ieee.org
 ... The **conditional access**, ie, the scrambling key distribution system, is discussed in Section III. ... K1 in (I), is seen as a **public key** (everyone is able to encrypt ...
 Cited by 266 - [Related articles](#) - [Web Search](#) - [BL Direct](#) - All 2 versions

Method and apparatus for providing **conditional access** in connection-oriented interactive networks ...

AH Wasilewski, DF Woodhead, GL Logston - US Patent App. 09/135,615, 1998 - [Google Patents](#)
 ... Methods and apparatus for applying **conditional access** are described that comprise encrypting ... encrypting the second key according to a **public-key** encryp- tion ...
 Cited by 31 - [Related articles](#) - [Web Search](#) - All 7 versions

[PDF] ► A Key Transport Protocol Based on Secret Sharing—An Application to **Conditional Access Systems**

AM Eskicioglu, T Multimedia - IS&T/SPIE's 13 th International Symposium on Electronic ... , 2001 - [Citeseer](#)
 ... A **conditional access** (CA) system 1,2 is a system ... 9 that eliminates the need for **public key** cryptography (or ... will explain how the required key **hierarchy** can be ...
 Cited by 4 - [Related articles](#) - [View as HTML](#) - [Web Search](#) - All 9 versions

Scrambling and key distribution scheme for digital television

W Kanjanarin, T Amornraksa - Ninth IEEE International Conference on Networks, 2001. ..., 2001 - ieeexplore.ieee.org
 ... Pay-TV service providers employ **Conditional Access** System (CAS), which uses scrambling, to ... There have been many proposals for key **hierarchy** models for key ...
 Cited by 13 - [Related articles](#) - [Web Search](#) - All 3 versions

Cryptographic authentication protocols for smart cards

LC Guillou, M Ugon, JJ Quisquater - Computer Networks, 2001 - [Elsevier](#)
 ... the verifier knows a **public key** corresponding to a ... cryptographic controls and card **hierarchy**; this history ... to the evolution of **conditional access**, resulting in ...
 Cited by 11 - [Related articles](#) - [Web Search](#) - All 3 versions

Verification of the source of program information in a **conditional access** system

HG Pinder, MS Paigon, GL Akins III, RO Banker - US Patent 6,105,134, 2000 - [Google Patents](#)
 ... A. Gardner [57] ABSTRACT A cable television system provides **conditional access** to services ... PIN EA **PUBLIC KEY** EAD \i ^HEADER -1502 hCAA FIELDS 1506 \- EA FIELDS ...
 Cited by 11 - [Related articles](#) - [Web Search](#) - All 2 versions

Nark: Receiver-based multicast non-repudiation and key management- ► psu.edu/for

B Briscoe, I Fairman - Proceedings of the 1st ACM conference on Electronic commerce, 1999 - portal.acm.org
 ... All the key **hierarchy** approaches send new keys over the multicast ... require each sender to authenticate their messages individually, **public key** signing leads to ...
 Cited by 25 - [Related articles](#) - [Web Search](#) - All 10 versions

Beyond cryptographic **conditional access**

DM Goldschlag, DW Kravitz - Proceedings of the USENIX Workshop on Smartcard Technology ..., 1999 - portal.acm.org

... of this bit-string with the **public key** of a ... For example, a **hierarchy** of signing authorities may exist ... work has been copy protection and not **conditional access**. ...

[Cited by 4](#) - [Related articles](#) - [Web Search](#) - [All 3 versions](#)

A prepositioned secret sharing scheme for message authentication in broadcast networks-

► [cuny.edu](#) (PDF)

AM Eskicioglu - Proceedings of the Communications and Multimedia Security ..., 2001 - books.google.com

... distributes, maintains and revokes **public-key** certificates. ... audio/video content in **conditional access** systems4 ... be used to establish the required key **hierarchy**. ...

[Cited by 6](#) - [Related articles](#) - [Web Search](#) - [All 7 versions](#)

Conditional access system

AJ Wasilewski, HG Pinder, GL Akins, MS Paigon - US Patent App. 09/881,428, 2001 - Google Patents

... 239; 725/31 (57) ABSTRACT A cable television system provides **conditional access** to services. ... 1502 -CAA FIELDS -1506 > EA FIELDS 1516 FIG-15 EA **PUBLIC KEY** EAD u ...

[Cited by 5](#) - [Related articles](#) - [Web Search](#) - [All 4 versions](#)

Secured Web access- ► [purdue.edu](#) (PDF)

M Mohania, V Kumar, Y Kambayashi, B Bhargava - Digital Libraries: Research and Practice, 2000 Kyoto, ..., 2000 - ieeexplore.ieee.org

... user is either given **conditional access**, timed access ... Such **hierarchy** is necessary in answering ... **Public key** cryptographic systems provide a more sophisticated ...

[Cited by 3](#) - [Related articles](#) - [Web Search](#) - [All 3 versions](#)

Source authentication of download information in a **conditional access system**

GL Akins, RO Banker, MS Paigon, HG Pinder, AJ ... - US Patent App. 09/748,313, 2000 - Google Patents

... 380/241; 380/239; 380/229 (57) ABSTRACT A cable television system provides **conditional access** to services ... 15H 1525-J PIN J FIG 15 1527-^ EA **PUBLIC KEY** -1506 JJ ...

[Cited by 2](#) - [Related articles](#) - [Web Search](#) - [All 8 versions](#)

Representing entitlements to service in a **conditional access system**

GL Akins, RO Banker, MS Paigon, HG Pinder, AJ ... - US Patent App. 09/930,901, 2001 - Google Patents

... CI 380/282 (57) ABSTRACT A cable television system provides **conditional access** to services. ... PIN EA **PUBLIC KEY** EAD 14 -HEADER -1502 •CAA FIELDS 1506 EA FIELDS ...

[Cited by 2](#) - [Related articles](#) - [Web Search](#) - [All 8 versions](#)

Public-key techniques: randomness and redundancy

LC Guillou, M Davio, JJ Quisquater - Cryptologia, 1989 - informaworld.com

Guillou, Davio, and Quisquater **Public-Key** Techniques: Randomness and Redundancy

PUBLIC-KEY TECHNIQUES: RANDOMNESS AND REDUNDANCY Louis C. Guillou W, Marc Davio ...

[Cited by 11](#) - [Related articles](#) - [Web Search](#)

Keeping card data secure at low cost

AW Vaidya, TSS Int - Security and Detection, 1995., European Convention on, 1995 - ieeexplore.ieee.org

... memory some logic circuitry giving **conditional access** and a ... the memory and decrypted using the appropriate **public key**. ... There is a **hierarchy** of functions that a ...

[Cited by 2](#) - [Related articles](#) - [Web Search](#) - [BL Direct](#) - [All 2 versions](#)

[PDF] ► Secure mediation: Requirements and design

J Biskup, U Fiegl, Y Karabulut - DATABASE SECURITY, 1999 - Citeseer

... otherwise. For the basic protocols we always only need the **public key** for encryption in credentials, as sketched in the following. ...

[Cited by 23](#) - [Related articles](#) - [View as HTML](#) - [Web Search](#) - [BL Direct](#) - [All 8 versions](#)

[\[PDF\] ► On the Security of Digital Video Distribution Systems](#)

A Adas, T Tran, AN Tantawy - 1996 - Citeseer

... the use of a key **hierarchy** where the ... any **public key** algorithms for authentication because of patent ... scrambling and the **conditional access** application reside on ...

[Related articles](#) - [View as HTML](#) - [Web Search](#) - [Library Search](#) - [All 2 versions](#)

[A Trusted Third Party Network for the Equi© rypt Access Control System](#)

AFA Teledetection - Global Information Infrastructure (GII) Evolution: ..., 1996 - books.google.com

... allowing a customized open **conditional access** system implementation. ... in which case the ACU's **public key** will be ... without a systematic **hierarchy** between TTPs. ...

[Related articles](#) - [Web Search](#)

[VERIFICATION OF THE SOURCE OF PROGRAM OF INFORMATION IN A CONDITIONAL ACCESS SYSTEM](#)

GL Akins III, RO Banker, MS Palgon, HG Pinder - EP Patent 1,010,323, 2001 - freepatentsonline.com

... 24 is a diagram showing the relationship between TEDs and the rest of **conditional access** system 601; ... 28 is a description of a **public key hierarchy**; and; FIG. ...

[Related articles](#) - [Web Search](#) - [All 5 versions](#)

[ENCRYPTION DEVICES FOR USE IN A CONDITIONAL ACCESS SYSTEM](#)

M PALGON, H PINDER - 1999 - freepatentsonline.com

... 24 is a diagram showing the relationship between TEDs and the rest of **conditional access** system 601; ... 28 is a description of a **public key hierarchy**; and; FIG. ...

[Related articles](#) - [Web Search](#) - [All 5 versions](#)

[AUTHORIZATION OF SERVICES IN A CONDITIONAL ACCESS SYSTEM](#)

GL Akins III, RO Banker, HG Pinder, AJ Wasilewski - EP Patent 1,000,508, 2001 - freepatentsonline.com

... 24 is a diagram showing the relationship between TEDs and the rest of **conditional access** system 601; ... 28 is a description of a **public key hierarchy**; and; FIG. ...

[Web Search](#) - [All 6 versions](#)

[CONDITIONAL ACCESS SYSTEM](#)

GL Akins III, MS Palgon, HG Pinder, AJ Wasilewski - EP Patent 1,000,511, 2001 - freepatentsonline.com

... 24 is a diagram showing the relationship between TEDs and the rest of **conditional access** system 601; ... 28 is a description of a **public key hierarchy**; and; FIG. ...

[Related articles](#) - [Web Search](#) - [All 5 versions](#)

[MARKS: Zero side effect multicast key management using arbitrarily revealed key sequences-](#)

[► ucl.ac.uk \(pdf\)](#)

B Briscoe - Lecture Notes in Computer Science, 1999 - Springer

... of approaches involves a single key for the multicast data, but a **hierarchy** of keys ... key can be sent to each of them encrypted with each **public key** using client ...

[Cited by 109](#) - [Related articles](#) - [Web Search](#) - [BL Direct](#) - [All 15 versions](#)

[Towards secure mediation](#)

J Biskup, U Fiegl, Y Karabulut - Workshop Sicherheit und Electronic Commerce, Essen, Germany, 1998 - Is6-www.informatik.uni-dortmund.de

... with (some of) the **public key(s)** occurring in ... **Conditional Access** Workshop, 44th RACE Concertation Meeting , Brussel ... Role **hierarchies** and constraints for lattice ...

[Cited by 10](#) - [Related articles](#) - [View as HTML](#) - [Web Search](#) - [All 6 versions](#)

[Key management for encrypted broadcast- ► tau.ac.il \(pdf\)](#)

A Wool - ACM Transactions on Information and System Security (TISSEC), 2000 - portal.acm.org
... General Terms: Security Additional Key Words and Phrases: **Conditional access**,
pay-per ... However, their techniques rely on RSA **public-key** cryptography [Rivest et ...
[Cited by 26](#) - [Related articles](#) - [Web Search](#) - [All 14 versions](#)

[PS] ► [A security platform for future telecommunication applications and services](#)
M Gehrke, E Koch - Proc. of the 6th Joint European Networking Conference, 1992 - igd.fhg.de
... relations between objects (eg **hierarchy** or federation ... frequency, such as **public key**
certificates, will ... the RACE Workshop on **Conditional Access**, Bruessel, Nov ...
[Cited by 5](#) - [Related articles](#) - [View as HTML](#) - [Web Search](#) - [All 3 versions](#)

[Method of electronic payment by chip card by means of numbered tokens allowing the detection of ...](#)
LC Guillou, JJ Quisquater - US Patent 5,305,383, 1994 - Google Patents
... For **conditional access**, keyholder cards are used. ... 15 which is beyond his control
Public-key algorithms will ... of the au- algorithms with a **hierarchy** of secret keys ...
[Cited by 10](#) - [Related articles](#) - [Web Search](#) - [All 2 versions](#)

[PDF] ► [Security protocols over open networks and distributed systems: Formal methods for their analysis, ...](#)
S Gritzalis, D Spinellis, P Georgiadis - Computer Communications, 1999 - eprints.kfupm.edu.sa
... the Equicrypt protocol [38] for **conditional access** to multimedia ... not cover protocols
using **public-key** algorithms nor ... Boyd proposes a **hierarchy** of extensional ...
[Cited by 86](#) - [Related articles](#) - [View as HTML](#) - [Web Search](#) - [All 12 versions](#)

[Protecting Intellectual Proprietary Rights Trough Secure Interactive Contract Negotiation-](#)
► [iscte.pt \(pdf\)](#)
C Serrão, J Guimarães - Lecture notes in computer science, 1999 - Springer
... allowing the integration of a **hierarchy** of effective ... the API, developers of **conditional**
access systems can ... through the use of **public key** cryptography and smart ...
[Related articles](#) - [Web Search](#) - [BL Direct](#) - [All 8 versions](#)

[Application data table for a multiservice digital transmission system](#)
F Rey, T Furet, P Poulain, P It - 2000 - freepatentsonline.com
... example, by a combined hash and **public key/private key** ... 2 shows the architecture of
the **conditional access** system of ... Figure 6 shows the **hierarchy** of packets for ...
[Web Search](#) - [All 7 versions](#)

[Method and apparatus for controlling access to confidential data by analyzing property inherent in ...](#)
RD Cassagnol, DM Dillon, DS Kloper, SJ Weber, BE ... - US Patent App. 09/160,846, 1998 - Google Patents
... For example, **conditional access** broad- casting networks such as cable television
networks and, more recently, direct satellite broadcasting networks are based ...
[Cited by 1](#) - [Related articles](#) - [Web Search](#) - [All 4 versions](#)

[Emerging Optical Network](#)
V Authors - 2000 - books.google.com
... customized application of mobile enhanced logic CAP competitive access provider
OR carrierless amplitude and phase modulation CAT **conditional access** table xvi ...
[Web Search](#)

[PDF] ► [Directory Enabled Policy Based Networking](#)
CM Kelilaa - 2001 - prod.sandia.gov
... As the names indicate, these represent a **hierarchy** of delegated administration. ...

application, and time of day, can be established for **conditional access**-control ...

[View as HTML](#) - [Web Search](#) - [All 5 versions](#)

Secure super distribution of user data

AAM Staring, FLAJ Kamperman - US Patent App. 10/011,889, 2001 - Google Patents
... title; [0022] a decryption key of the user data, encrypted in the **public key** of the ... invention one or more keys, which can be part of a key **hierarchy**, are used ...

[Web Search](#) - [All 6 versions](#)

Threshold cryptography scheme for message authentication systems

A Eskicioglu - US Patent App. 09/961,901, 2001 - Google Patents

... of the sender's **public key** is a major problem requiring complex **public key** infrastructures. ... secret sharing may be used to establish the required key **hierarchy**. ...

[Related articles](#) - [Web Search](#) - [All 7 versions](#)

Baseband Signal Processing

E Saggese - Satellite Communication Systems Design, 1993 - books.google.com

Page 99. Baseband Signal Processing E. Saggese I. Introduction 3 This chapter is devoted to operations performed on the baseband ...

[Related articles](#) - [Web Search](#)

Creating a new security for tomorrow's communication networks and information systems

M Riguidel - Annals of Telecommunications, 2000 - Springer

... ISAKMP (RFC2408). See www.ietf.org/html.charters/ipsec-charter.html. 12.

PKIX : PVd X509 : **Public-Key** Infrastructure x.509. The PKEX ...

[Cited by 2](#) - [Related articles](#) - [Web Search](#) - [BL Direct](#) - [All 3 versions](#)

Unified end-to-end security methods and systems for operating on insecure networks

MM Atalla - US Patent 5,960,086, 1999 - Google Patents

... 1, XP000428048 Tsubakiyama H et al: "Security for Information Data Broadcasting System with **Conditional-Access** Control" see p. 165, right-hand col. ...

[Cited by 5](#) - [Related articles](#) - [Web Search](#) - [All 7 versions](#)

System for generation of object profiles for a system for customized electronic identification of

...

FSM Herz, JM Eisner, LH Ungar - US Patent 5,835,087, 1998 - Google Patents

... 58-67. Rivest, RL; Shamir, A. & Adleman, L.; "A Method for Obtaining Digital Signatures and **Public-Key** Cryptosys- tems", Communications of the ACM, Feb. ...

[Cited by 114](#) - [Related articles](#) - [Web Search](#) - [All 2 versions](#)

System for customized electronic identification of desirable objects

FSM Herz - US Patent 6,029,195, 2000 - Google Patents

Page 1. United States Patent Herz US006029195A [ii] Patent Number: [45] Date of Patent: 6,029,195 Feb. 22, 2000 [54] SYSTEM FOR CUSTOMIZED ...

[Cited by 115](#) - [Related articles](#) - [Web Search](#) - [All 4 versions](#)

System for generation of user profiles for a system for customized electronic identification of ...

FSM Herz, JM Eisner, LH Ungar, MP Marcus - US Patent 5,754,939, 1998 - Google Patents

... 58-67. Rivest, RL; Shamir, A. & Adleman, L.; "A Method for Obtaining Digital Signatures and **Public-Key** Cryptosys- tems". Communications of the ACM. Feb. 1978. ...

[Cited by 138](#) - [Related articles](#) - [Web Search](#) - [All 2 versions](#)

Method for granting accesses to information in a distributed computer system

A Duncan, S Farrell, C Scott - US Patent 6,163,844, 2000 - Google Patents

... SGML documents are sequence of characters that are physically organized as a set of entities and are logically organized in a **hierarchy** of elements. ...

[Cited by 5](#) - [Related articles](#) - [Web Search](#) - [All 2 versions](#)

[BOOK] [SEMPER--secure Electronic Marketplace for Europe](#)

G Lacoste - 2000 - [books.google.com](#)

... Electronic Commerce 81.3.1 Secure Channels 81.3.2 Trusted Market Provider 91.3.3 Digital Signatures and **Public-Key** Infrastructures 10.6.1 Class **Hierarchy** 174 ...

[Cited by 25](#) - [Related articles](#) - [Web Search](#) - [Library Search](#) - [All 3 versions](#)

[Pseudonymous server for system for customized electronic identification of desirable objects](#)

FSM Herz, JM Eisner, M Salganicoff - US Patent 5,754,938, 1998 - [Google Patents](#)

... 58-67. Rivest, RL; Shamir, A & Adleman, L.; "A Method for Obtaining Digital Signatures and **Public-Key** Cryptosystems". Communications of the ACM. Feb. 1978. ...

[Cited by 75](#) - [Related articles](#) - [Web Search](#) - [All 2 versions](#)

[PDF] [► Commercial electronic publishing over open networks: a global approach based on mobile objects \(...](#)

JH Morin - 1999 - [cul.unige.ch](#)

Page 1. UNIVERSITÉ DE GENÈVE Faculté des Sciences Économiques et Sociales Département de Systèmes d'Information Commercial Electronic Publishing ...

[Cited by 12](#) - [Related articles](#) - [View as HTML](#) - [Web Search](#) - [Library Search](#) - [All 5 versions](#)

[PDF] [► Pre-study on "Customer Care, Accounting, Charging, Billing, and Pricing"](#)

B Stiller, G Fankhauser, B Plattner, N Weiler - Computer Engineering and Networks Laboratory TIK, ETH ..., 1998 - [tik.ee.ethz.ch](#)

... As an example, critical enabling technologies for Internet Electronic Commerce, such as hardware and software in the **public key** infrastructure, eg, smart ...

[Cited by 5](#) - [Related articles](#) - [View as HTML](#) - [Web Search](#) - [All 5 versions](#)

[STREAMING MEDIA PLAYER WITH CONTINUOUS CONTROL AND PROTECTION OF MEDIA CONTENT](#)

TG Shamoon, RD Hill, CD Raddcliffe, JP Hwa, P It - 2000 - [freepatentsonline.com](#)

... eg, message authentication codes), digital signatures, and/or **public key** certificates used ... indicators allow IPMP System 812 to establish a **hierarchy** of messages ...

[Web Search](#) - [All 4 versions](#)

Key authors: [B Macq](#) - [J Quisquater](#) - [B Briscoe](#) - [F Herz](#) - [A Wasilewski](#)

"public key" "conditional access" hierarchy

[Go to Google Home](#) - [About Google](#) - [About Google Scholar](#)